UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DISTRICT

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	No. 4:16-CR-258 CEJ (NAB)
	)	
ALDEN DICKERMAN,	)	**FILED UNDER SEAL**
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S SUPPLEMENTAL MOTION TO SUPPRESS EVIDENCE AND STATEMENTS

COMES NOW the United States of America, by and through its attorneys, Richard G. Callahan, United States Attorney for the Eastern District of Missouri, and Colleen Lang, Assistant United States Attorney for said district, and files its Response to Defendant's Supplemental Motion to Suppress Evidence.

I. INTRODUCTION

Defendant filed a supplemental motion to suppress evidence seized by law enforcement officers. Defendant specifically claims in this motion that law enforcement's search and seizure of data and electronic communications on Freenet is an illegal search under the Fourth Amendment and violated defendant's Constitutional privacy rights. Defendant also alleged broad violations of the Electronic Communications Privacy Act and the Stored Communications Act.

The law enforcement's collection of basic data on Freenet, an open-sourced peer-to-peer file-sharing software program on the Internet, is not an illegal search nor seizure. The

information collected by law enforcement is not an interception of content information nor is it private communications. However, even if it were considered an interception content information, the law enforcement node on Freenet is a party to the communication with the defendant. Neither the Electronic Communications Privacy Act nor the Stored Communications Act apply to this case.

II. FACTUAL BACKGROUND[1]

A. Background on Freenet and Law Enforcement Investigations on Freenet

In September of 2011, Special Investigator ("S.I.") Wayne Becker of the Dent County Sheriff's Department began to collect "keys" and files of child pornography located and being shared on "Freenet." In April of 2012, Special Investigator ("S.I.") Wayne Becker of the Dent County Sheriff's Department began to review logs as a peer node on Freenet for requests of files containing child pornography. SI Becker had located the keys of known child pornography files from publicly posted sites or message boards on the Freenet network. Freenet is a type of peer-to-peer network software that allows users to share files over the Internet. Freenet is "open-sourced," meaning the source code for the software is "open" and, thus, maybe modified by users to a certain extent. It uses a decentralized, distributed data store to keep and deliver information. It is free and publicly available software for publishing and communicating on the Internet. Freenet's focus is to provide a place on the Internet for free speech and anonymity. In Freenet, each file is made up of several blocks, or splits, that are stored independently of each other. To view a file, you must request all the blocks that are necessary to reconstruct it. The keys used to identify a block to retrieve are the hash values of

[1] The background and factual summary information provided is intended as a general guide to aid the Court. It is not intended as a comprehensive statement of the government's case.

the blocks. Users contribute to the network by giving bandwidth and a portion of their hard drive for storing files. Freenet transmits data between nodes, also known as peers. Freenet also stores data on the nodes. The process of finding a piece of data, or a place to store data, is called routing. Nodes are the computers running Freenet. A node in Freenet interacts directly with its directly connected peers. Each peer's IP address is visible to a node, but a node does not learn the IP addresses of its peers' peers. On the current version of Freenet, a node may have up to 142 peers. (See Exhibit 1, "Statistical Detection of Downloaders of Child Exploitation Materials in Freenet" for more detail on Freenet). When making a request for a file on Freenet, the request goes to the user's peers' nodes. Those peers check to see if they have any parts of the requested file (known as "blocks"). If they do, they send the block to the initial requestor. If the peer does not have the requested block, it will decrement the HTL[2] and then forward the request to one its peers. When a node receives a request, it only knows of the immediate node from which the request was received. (Exhibit 1, Section 4.2, page 5).

Researchers and law enforcement studied the Freenet open source code and analyzed activity on Freenet. Through their study they were able to create a statistical algorithm to determine the likelihood that a peer is the requestor of child pornography files, versus being a peer that only relayed the request. The timeline for these activities are as follows. Beginning in 2012, S.I. Becker collected keys in order to build database of files on Freenet that are associated with known or suspected child pornography images and videos. Researchers at the

[2] When a Freenet node requests a block it sends the request to one of its peers. If the peer does not have the block in its' storage, the peer requests the block from one of its own peers, and so forth. If a block is no longer in the network, the requests between peers could be forwarded on indefinitely. To prevent that, Freenet uses a "hops to live" ("HTL") counter. The HTL begins at a value of 18 and is decremented by each relay node until the value is zero. When that happens a "not found" message is relayed back through the requesting chain of nodes. (Ex. 1, Section 2.2, page 3).

University of Massachusetts Amherst helped modify the open sourced Freenet program for law enforcement use. The modification logs the IP address, the content hash key values, the HTL, types of requests, and the date/time of the requests that the node receives. Anyone using Freenet can make certain modifications to its open source code to collect information, like law enforcement has done.

S.I. Becker began investigating child pornography offenders on Freenet in 2012 and 2013. In 2014, the research staff at University of Massachusetts Amherst worked with SI Becker to develop a new method to determine if an IP address appeared to be requesting known child pornography files on Freenet.

In 2015, these researchers developed a statistical algorithm for determining whether a peer is more likely to be requesting child pornographic material on Freenet or relaying such a request. This algorithm was still being refined at the time of S.I. Becker's investigation into the Defendant's requests for child pornography on Freenet. At the time of the investigation into the Defendant, S.I. Becker was using a method that is fundamentally similar to what the algorithm does now because both methods count requests for blocks that make up a file of known child pornography. A count of requests distinguishes the requesters from relayers.

While Freenet tries to be a harbor for anonymity, the website warns about the possibility that an IP address could be recognized. The website states, "If you are connected to a node, and can recognise the keys being requested (probably because it was posted publicly), you can show statistically that the node in question probably requested it, based on the proportion of the keys requested from that node, the locations of nearby nodes, the HTL on the

requests and so on.[3]" The warning is basically what law enforcement is doing – recognizing known keys and determining whom is a requestor versus a relayer by the number of blocks being requested.

B. Instant Offense

While investigating Freenet requests on April 2, 2015, S.I. Becker came across a computer with an IP address in the state of Missouri that requested a file of known child pornography. S.I. Becker documented the data related to that IP address' request for the file of child pornography on Freenet. Exhibit 2, S.I. Becker's Excel Spreadsheet. The collection of this data (which includes the IP address, hash key values of the file being requested, the date and time of the request) is not intercepted by the S.I. Becker. He collects the data as it comes to his node on Freenet from the Defendant whom is his peer on Freenet. The data is coming to a law enforcement node unsolicited. S.I. Becker collected the file and IP address information and sent it to Det. Michael Slaughter of the St. Louis County Police Department, who sent a subpoena to AT&T Internet services to determine the subscriber information for that IP address. AT&T responded that the name and address of the subscriber was Janis Dickerman at 9524 Corregidor Drive, St. Louis, Missouri, 63134.

A search warrant was prepared by Det. Slaughter and signed by St. Louis County Judge Borbonus on August 18, 2015. The search warrant stated "While reviewing requests received by undercover Freenet nodes, located in Missouri, S.I. Becker observed IP address 172.12.235.62 routing/or requesting suspected child pornography blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent

[3] Warning from the Freenet Project webpage (https://wiki.freenetproject.org/FAQ).

original requestor of the file." Exhibit 3, Search Warrant Affidavit, ¶ 6. "S.I. Becker observed that on April 2, 2015, between 11:08 p.m. UTC and 11:10 p.m. UTC, a computer running Freenet software, at IP address 172.12.235.62, requested from Freenet law enforcement nodes 69 parts, or blocks, of the following file." Ex. 3, ¶ 7. The affiant then identified that file with its' name and unique SHA1 hash value. The file was then described as a folder containing seventeen (17) images of child pornography.

The search warrant was executed by St. Louis County Police on August 18, 2015, at 9524 Corregidor Drive, St. Louis, Missouri. The Defendant, Alden Dickerman, was the only person home during the execution of the warrant. The Defendant admitted to having used Freenet in the past before invoking his *Miranda* rights. Computers were seized from the home and were searched by S.I. Becker. S.I. Becker determined that the Defendant's Asus laptop contained Freenet software and files of child pornography.

On June 22, 2016, a federal grand jury indicted the Defendant on one count of Possession of Child Pornography in violation of Title 18 U.S.C. Section 2252(a)(5)(B).

III. LEGAL ANALYSIS

A. Defendant Does Not Have A Legitimate Expectation of Privacy on Freenet; Information Logged by Law Enforcement was Not an Unlawful Search or Seizure; Law Enforcement was a Party to the Communication

Defendant argues that he had a legitimate expectation of privacy in his requests on Freenet. The defendant did not have a reasonable expectation of privacy in his requests on Freenet because he was sending the requests for these files out to peers on Freenet, who are complete strangers. The defendant attempts to rely on *Kyllo v. United States*, 533 U.S. 27

(2001); *United States v. Jones*, 565 U.S. 400 (2012): and *Florida v. Jardines*, 133 S.Ct. 1409 (2013). The Supreme Court in *Kyllo* stated,

> [w]e have subsequently applied this principle to hold that a Fourth Amendment search does *not* occur—even when the explicitly protected location of a *house* is concerned—unless "the individual manifested a subjective expectation of privacy in the object of the challenged search," and "society [is] willing to recognize that expectation as reasonable." *Ciraolo, supra,* at 211, 106 S.Ct. 1809. We have applied this test in holding that it is not a search for the police to use a pen register at the phone company to determine what numbers were dialed in a private home, *Smith v. Maryland*, 442 U.S. 735, 743–744, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), and we have applied the test on two different occasions in holding that aerial surveillance of private homes and surrounding areas does not constitute a search, *Ciraolo, supra; Florida v. Riley*, 488 U.S. 445, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989). *Id* at 33.

The cases the defendant relied on, *Kyllo, Jones,* and *Jardines,* all involved a search of a person's home or car. In this case, the defendant is on the Internet, a publicly available space, making requests to strangers. The technology used to collect data by law enforcement is not invading his home or his property. It is not even surveilling the defendant's property in anyway. The defendant sent requests for files to the law enforcement Freenet node. The law enforcement node on Freenet merely gathers the information associated with the requests it receives before making a new request to its' peers on Freenet for the file or returning the requested block, if it had the block. The law enforcement node is a party to the defendant's communication on Freenet.

i. <u>No Legitimate Expectation of Privacy when Sending Freenet Requests to Unknown Peers on the Network.</u>

Katz vs. United States, 389 U.S. 347 (1967), discusses distinguishing between what an individual has "knowingly exposed to the public" and "what he seeks to preserve as private, even in an area accessible to the public," when determining whether Fourth Amendment protections apply. *Id.* at 353. In this case, the defendant is knowingly exposing his

communications when downloading a file on Freenet, because his requests are then sent to his peer nodes on Freenet, which are computers of unknown peers. Those peers have to determine whether they have any of the blocks that makeup the file, and if they do not, they then request it from their peers. The defendant's requests, or "communications" as the defendant defines it, are no longer confined to his home, work, car, or even his own computer. The defendant's request, or communication, are out on the Internet for any Freenet node that receives it to view.

ii. Freenet Warns Users that IP Addresses Can be Recognized by a Peer Node

The defendant alleged that he had an actual and subjective belief in Freenet's service to maintain his anonymity and privacy, but Freenet warns it users that the network is not completely anonymous. On their website, Freenet warns its users about the possibility that an IP address could be recognized. The website states, "If you are connected to a node, and can recognise the keys being requested (probably because it was posted publicly), you can show statistically that the node in question probably requested it, based on the proportion of the keys requested from that node, the locations of nearby nodes, the HTL on the requests and so on.[4]" The warning is basically what law enforcement is doing – recognizing known keys and determining whom is a requestor versus a relayer by the number of blocks being requested.

Defendant further alleged that he intentionally used Freenet to protect his privacy interests in his communications. Freenet is a free software that can been found on the Internet. It was created by Ian Clarke, as his final year project, when he was a student at the University of Edinburgh. His goal behind the Freenet project was to create a platform for freedom of

[4] Warning from the Freenet Project webpage (https://wiki.freenetproject.org/FAQ).

speech with strong anonymity protection, however, Freenet offers no guarantees that it is one hundred percent anonymous, and even warns users that it is not. Also, there are two modes of operation on Freenet: opennet and darknet. In opennet, nodes connect users to any other Freenet user. In darknet mode, the user only connects to peers to which the user has explicitly given permission. Ex. 1, Section 2, p. 2. The defendant was using opennet mode, and therefore opening up his communications to any other Freenet user.

Relevant to the discussion about privacy on Freenet are recent cases around the country that have found users of the Tor network[5] have no reasonable expectation of privacy in their IP addresses. Similar to Freenet, the Tor network is attractive to users looking for anonymity because the Tor network attempts to make a user's IP address more difficult to discover. "It is clear to the Court that Defendant took great strides to hide his IP address via his use of the Tor network. However, the Court finds that any such subjective expectation of privacy—if one even existed in this case—is not objectively reasonable. SA Alfin testified that when a user connects to the Tor network, he or she must disclose his or her real IP address to the first Tor node with which he or she connects. This fact, coupled with the Tor Project's own warning that the first server can see 'This IP address is using Tor,' destroys any expectation of privacy in a Tor user's IP address." *United States v. Matish*, 2016 WL 3545776 (E.D. Va. June 23, 2016).

[5] The U.S. Naval Research Laboratory created the Tor network in an attempt to protect government communications. The public now can access the Tor network. Many people and organizations use the Tor network for legal and legitimate purposes; however, the Tor network also is replete with illegal activities, particularly the online sexual exploitation of children.
A person can download the Tor browser from the Tor website. See Tor Project: Anonymity Online, https://www.torproject.org (last visited May 23, 2016). SA Alfin testified that the Tor network possesses two primary purposes: (1) it allows users to access the Internet in an anonymous fashion and (2) it allows some websites—hidden services—to operate only within the Tor network. Although a website's operator usually can identify visitors to his or her site through the visitors' Internet Protocol ("IP") addresses, Tor attempts to keep a user's IP address hidden. *United States vs. Matish*, 2016 WL 3545776.

"Although the Tor network hides IP addresses, the 'Tor network does not strip users of all anonymity' and to access the network users 'must still send and receive information, including IP addresses, through another computer, such as an Internet Service Provider . . . The FBI was ultimately able to locate Henderson by tracking his IP address to his internet provider, demonstrating that Henderson voluntarily turned his IP address information to this third party so that it could provide him with web services." *United States v. Henderson*, No. 15-cr-00565-WHO-1, 2016 WL 4549108, *5 (N.D. Cal. Sep. 1, 2016).

Based on the warnings from Freenet, plus the nature of how the requests on Freenet are made on opennet, the defendant had no actual reasonable expectation that his requests on Freenet were completely anonymous and private. While networks, like Freenet and Tor, attempt to be a harbor for free speech and anonymity, these networks cannot make users completely anonymous since the user has to send communication requests, that included their IP address, to another user. Users of these networks cannot have a subjective expectation of privacy when they are sharing information and communication with third parties. Further, since Freenet users are sharing their requests with another user, in this case an undercover law enforcement node, the do not have a legitimate expectation of privacy.

iii. Law Enforcement is not Searching or Seizing Private or Protected Communications; Law Enforcement is a Party to the Communication

In *Smith v. Maryland*, 442 U.S. 735, (1979), the Supreme Court held that telephone numbers dialed from a particular home do not have a "legitimate expectation of privacy" in the numbers dialed, while the contents of the communications do. In this case, the requests sent out on Freenet are similar to a number being dialed. The defendant sent a request for a certain file similar to a person dialing a certain telephone number. The key hash value is collected is

like collecting a phone number. Law enforcement is not intercepting anything, since the communications are coming to them, as a peer node on Freenet. Law enforcement are passively sitting on Freenet collecting data from requests specifically directed to them unsolicited. There is no law enforcement search happening. SI Becker is collecting communications he received that were disclosed and directed to him. SI Becker can analyze information that was directed and sent to him on Freenet.

The requests are not analogous to email in the way that the defense contends. There is no correspondence to read or photograph to look at - it is a mere data is coming to the law enforcement node from other peer nodes. Email users do have a reasonable expectation of privacy in their emails in many circumstances, but the that expectation of privacy does not matter in this case. Since the receiver of an email, as a party to the communication, can use that email as they please. If person sends an email to an undercover police officer, then that officer's use of that email is not a constitutional or statutory violation because the officer was a party to the communication. This is the same on Freenet, the undercover law enforcement node is the receiver of the information directed to him by the defendant. Then the law enforcement node can collect and log that communications since it was directed to him.

The defendant misplaced his trust when he sent his file request to the undercover law enforcement node on Freenet. Similar to the situation in *Hoffa vs. United States*, 385 U.S. 293, (1966), the defendant was relying upon his misplaced confidence that his friend would not reveal his wrong doing, when the friend was in fact an undercover government informant. The Supreme Court in *Hoffa*, stated that, "[n]either this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a

person to whom he voluntarily confides his wrongdoing will not reveal it." *Id.* at 302. Therefore, the defendant cannot rely on Fourth Amendment protections when the requests he was sending out to other peer nodes, turn out to be an undercover law enforcement node.

iv. Current Case Law Regarding Searches on Similar Peer-to-Peer Networks

Courts have rejected the argument that individuals have a reasonable expectation of privacy when using file sharing software. While the government was unable to located any cases that discuss the Freenet program specifically, below are several relevant cases dealing with similar peer-to-peer file sharing networks.

The Eighth Circuit Court of Appeals in *United States v. Stults*, 575 F3d 834, (8th Cir. 2009) addressed the issue of a person's expectation of privacy on peer-to-peer networks. The Eighth Circuit Court of Appeals followed several other federal courts and found that an individual does not have a reasonable expectation of privacy on a peer-to-peer file sharing network.

> Several federal courts have rejected the argument that an individual has a reasonable expectation of privacy in his or her personal computer when file-sharing software, such as LimeWire, is installed. *See, e.g., United States v. Ganoe,* 538 F.3d 1117, 1127 (9th Cir.2008) (holding that the defendant lacked a reasonable expectation of privacy in the downloaded files stored on his computer, meaning that an agent's use of a file-sharing software program to access child pornography files on the computer did not violate the defendant's Fourth Amendment rights); *United States v. Perrine,* 518 F.3d 1196, 1205 (10th Cir.2008) (holding that defendant had no expectation of privacy in government's acquisition of his subscriber information, including his IP address and name from third-party service providers, where the defendant voluntarily transmitted such information to Internet providers and enabled P2P file sharing on his computer, which permitted anyone with Internet access the ability to enter his computer and access certain folders); *United States v. Barrows,* 481 F.3d 1246, 1249 (10th Cir.2007) ("[The defendant] claims that he invited no one to use his computer and therefore expected its contents to remain private. Yet he surely contemplated at least some third-party

> access: he knowingly networked his machine to the city computer for the express purpose of sharing files."); *United States v. Brese*, No. CR–08–52–D, 2008 WL 1376269 (W.D.Okla. April 9, 2008) (unpublished) ("The Court finds that, notwithstanding any subjective expectation that Defendant may have had in the privacy of his computer, it was not reasonable for him to expect privacy in files that were accessible to anyone else with LimeWire (or compatible) software and an internet connection."); *United States v. Borowy*, 577 F.Supp.2d 1133, 1136 (D.Nev.2008) ("In this case, [the defendant] did not have a legitimate expectation of privacy in files he made available to others using P2P software."). *Id.* at 842-43

In *Stults*, the peer-to-peer network software in question was LimeWire[6]. And while LimeWire works a little differently than Freenet, an analogy can be made between the two. Both programs allow users to share files. In both programs, a user is requesting files from unknown users on the same network. The Eighth Circuit Court of Appeals in *Stults* found no reasonable expectation of privacy of a user on a peer-to-peer network.

> We hold that Stults had no reasonable expectation of privacy in files that the FBI retrieved from his personal computer where Stults admittedly installed and used LimeWire to make his files accessible to others for file sharing. One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking. As a result, "[a]lthough as a general matter an individual has an objectively reasonable expectation of privacy in his personal computer, we fail to see how this expectation can survive [Stults's] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program." *Ganoe,* 538 F.3d at 1127 (internal citation omitted). Even if we assumed that Stults "did not know that others would be able to access files stored on his own computer," Stults did know that "he had file-sharing software on his computer; indeed, he admitted that he used it—he says to get music [and to download pornography]." *Id.* As a result, Stults "opened up his download folder to the world, including Agent [Cecchini]." *Id.* "Having failed to demonstrate an expectation of privacy that society is prepared to accept as reasonable, [Stults] cannot invoke the protections of the Fourth Amendment." *Id.* at 843.

---

[6] LimeWire is a computer file-sharing program that any user could download for free over the Internet. LimeWire and similar programs connect network participants directly and allow them to download files from one another. To download a file, a LimeWire user opens the application and inputs a search term. LimeWire then displays a list of files that match the search terms and that are available for download from other LimeWire users. When a user downloads a file using the LimeWire network, he or she causes a digital copy of a file on another user's computer to be transferred to his or her own computer. *Stults* at 842.

When conducting an investigation into child pornography activities on LimeWire, the FBI had to actually retrieve files from the target. What law enforcement is doing on Freenet is even less of an intrusion, since law enforcement is merely collecting data that is coming to them. There is no reasonable expectation of privacy for users of peer-to-peer networks, including Freenet.

The Sixth Circuit Court of Appeals held in *United States v. Connor*, 2013 WL 1490109, 521 Fed. Appx. 493 (6th Cir. 2013)(unpublished) that a user of a file sharing program does not have a legitimate expectation of privacy. The Court in *Connor* further reasoned that sharing files on peer-to-peer networks is different from sending an email or a letter.

> Conner argues that under *United States v. Warshak*, 631 F.3d 266 (6th Cir.2010) (*en banc*), third-party access to information on one's computer is consistent with a reasonable expectation of privacy in that information. In *Warshak*, we agreed that the government could not compel a commercial ISP to turn over the contents of a subscriber's e-mails without a warrant because subscribers "enjoy a reasonable expectation of privacy in the contents of emails," even though an ISP has the ability to view the contents of e-mail prior to delivery. 631 F.3d at 288. In the context of e-mail, ISPs are "the functional equivalent of a post office or a telephone company," and like an ISP, both of these entities have the ability to intrude on the contents of messages in the course of delivering them to their intended recipients. *Id.* at 286. Since the right or ability of third parties to intrude on phone calls and letters has not been deemed sufficient to defeat a reasonable expectation of privacy in those modes of communication, we agreed that "it would defy common sense to afford emails lesser Fourth Amendment protection" than telephone calls or letters. *Id.* at 285–86.
>
> *Warshak* does not control this case because peer-to-peer file sharing is different in kind from e-mail, letters, and telephone calls. Unlike these forms of communication, in which third parties have incidental access to the content of messages, computer programs like LimeWire are expressly designed to make files on a computer available for download by the public, including law enforcement. Peer-to-peer software users are not mere intermediaries, but the intended recipients of these files. Public exposure of information in this manner defeats an objectively reasonable expectation of privacy under the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *see also California v. Greenwood*, 486 U.S. 35, 40–41, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988) (finding no reasonable expectation of privacy in "plastic garbage bags left on or at the side of a public street," which are accessible by "members of the public" and left

> on the curb "for the express purpose of conveying [them] to a third party, the trash collector").
>
> Conner responds that he did not know the files he downloaded from LimeWire would be publicly accessible. To prove this point, he emphasizes efforts he made to keep these files private by moving them to compact disks and reinstalling his operating system on the computer to "wipe the hard drive clean." But these efforts only prove that he was ineffective at keeping the files he downloaded from LimeWire from being detected. They do not establish that he was unaware of a risk of being discovered. As the Ninth Circuit observed when confronted with a similar argument, Conner's "subjective intention not to share his files d[oes] not create an objectively reasonable expectation of privacy in the face of [the] widespread public access" to his files LimeWire created. *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir.2010) (rejecting Fourth Amendment privacy claim of defendant who unsuccessfully attempted to use LimeWire's privacy features "to prevent others from downloading or viewing the names of files on his computer"). *Connor* at 488 -498.

Also similar to the allegations of the defendant in the case at hand, in *U.S v. Gabel* 2010 WL 3927697 (S.D. Fla. 2010)(unpublished), the defendant alleged that the users on peer-to-peer networks have a reasonable expectation of privacy in their files, thereby protecting them from warrantless searches by law enforcement using enhanced computer programs unavailable to the general public. Magistrate Judge Goodman declined to agreed and found the following, which the District Court adopted,

> The enhanced law enforcement software used in this case did not search any areas of Gabel's computer, download any files, or otherwise reveal any information that was unavailable to ordinary internet users. *Cf. Kyllo v. United States*, 533 U.S. 27, 40, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (holding that when law enforcement "uses a device that is not in general public use, to explore details ... *that would previously have been unknowable* without physical intrusion, the surveillance is a 'search.' ") (emphasis added). Rather, the enhanced software allowed law enforcement to gather and evaluate publically available information with greater efficiency and with an eye towards obtaining probative and admissible evidence of criminal activity.
>
> The Undersigned agrees with every other federal court to have addressed this issue, and finds that users of peer-to-peer networks do not enjoy a reasonable, objective expectation of privacy in the files they share. The Undersigned also agrees with the Ninth Circuit's view in *Borowy* that law enforcement's use of a computer program which allows them to confirm whether the files contain child pornography has no bearing on whether defendants possess a legitimate expectation of privacy in those pornographic files.

> Any of the hundreds of thousands (or millions) of users on the Gnutella network could have searched for Gabel's shared files and downloaded those files exclusively from Gabel. That is exactly what law enforcement did here.
>
> The enhanced programs merely permitted law enforcement to more easily organize and classify information that was otherwise available to the public, which aided them in obtaining evidence to support a search warrant. Gabel had no reasonable expectation of privacy in his files. He was, essentially, sharing them with the entire world. *Anyone* with internet access could have easily downloaded Gnutella client software, logged onto the network and downloaded Gabel's files. The fact that law enforcement did so with a device that enabled them to screen for child pornography and collect data for evidentiary purposes does not alter the privacy analysis or in any way shroud Gabel with the Fourth Amendment's protection. It simply means that the police were doing their job. The tool used by law enforcement here is no different, from a constitutional perspective, than the myriad special means—street cameras, radar and canines—that police legally use every day without prior judicial approval to efficiently gather evidence by accessing public information. These police tools do not generate Fourth Amendment concerns because they do not access anything which the public cannot access. Thus, law enforcement's use of an enhanced computer program is the digital equivalent of a pole camera, which is legal and which does not require a warrant or court order. *Id.* 2010 WL 3927697 (September 16, 2010), Report and Recommendations of Defendant's Motion to Suppress in 10-60168 Sept. 16, 2010 United States District Court for the Southern District of Florida. Adopted by the District Court, Court of Appeals denied to hear argument.

Another similar case from the United States District Court in Vermont is *United States v. Thomas*, where the defendants alleged that law enforcement obtained private information through a warrantless search on a peer-to-peer network. 2013 WL 6000484 (November 8, 2013). The Court found that, "either intentionally or inadvertently, through the use of peer-to-peer file sharing software, Defendants exposed to the public the information they now claim was private." *Id.* at 17. Further the Court stated that, "because there is no evidence that law enforcement's use of automated software reached information on Defendants' computers that was not made available for sharing by the public, Defendants' motions to suppress on the basis of a warrantless search in violation of the Fourth Amendment must be denied." *Id.* at 20.

The current case law around the country does not support the defendant's position. Courts have been ruling that: 1) individuals do not have a reasonable expectation of privacy on peer-to-peer file sharing networks; 2) file sharing on peer-to-peer networks is different than sending emails or other protected communication; and 3) law enforcement can use enhanced or modified software to locate individuals sharing child pornography files on peer-to-peer networks.

v. Third Party Expectation of Privacy

In *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court developed a bright-line application of the reasonable-expectation-of-privacy test that is relevant here. In what has come to be known as the "third-party doctrine," the Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties ... even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 743-44 (citing *Miller*, 425 U.S. 435,442-44). [7]

On Freenet, the request from the defendant for a file is intended for his peer nodes. Those nodes are parties to the communication, in this case the communication is a request for a file. Those nodes then must look at the request - including the key - and decide if it has the

[7] Also see cases where Courts have found that a defendant does not a legitimate expectation of privacy when he shares files of child pornography online with "friends." In *United States v. Brooks*, 2012 WL 6562947, the Court noted that a defendant has even less of an objective expectation of privacy when he, the user, "friends" the undercover agent and makes files available to that undercover officer. The court explained that if an individual assumes the risk that one of his "friends" would alert law enforcement about his trading child pornography, certainly that individual assumes the same risk when one of his "friends" actually is a law enforcement officer. *See Soderholm*, 2011 WL 5444053 at 7. As cautioned by the Supreme Court in *United States v. White*, 401 U.S. 745, 752 (1971), "[i]nescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police."

requested block. If it doesn't, the node generates a new request and sends it to another node, a peer node. Since it is a new request being generated as opposed to a routing of the original request, the Freenet node must extract the requester's IP address and retain it, along with the key. The defendant's allegation that the node receives the request in order to route it to another node is not completely accurate, the node first had to check to see if it has the block (or part of the file) and then creates a new request to send to its' peer nodes. Thereby making the law enforcement node a party to the communication, and thus, the defendant does have not a legitimate expectation of privacy in the information he voluntarily turned over to a third party.

In summary, the defendant's request for a certain file of child pornography are not intercepted by law enforcement. In fact, the request is directed at law enforcement node, since they are one of defendant's peers on the network. As a party to the communication, law enforcement can log the data associated with the request. Users of peer-to-peer networks do not have a reasonable expectation of privacy when file sharing.

B. Law Enforcement's Collection of Open Source Data on Freenet is Not in Violation of the Electronic Communications and Protection Act nor the Stored Communications Act.

i. Electronic Communications Privacy Act Does Not Apply

The defendant alleged in the second half of his supplemental motion that law enforcement's use of a modified version of Freenet to log IP address, key, date and time of requests without prior judicial authorization is in violation of the Electronic Communications Privacy Act ("ECPA"). This act is codified under Title 18 U.S.C. § 2510-22. Law enforcement in this case did not violate the ECPA because they did not intercept any contents

of the defendant's electronic communications on Freenet. The communication came directly to the law enforcement node. Further, even the if Court finds that defendant's electronic communication collected by law enforcement on Freenet was intercepted, the law enforcement node was a party to the communication, thereby excepting them from liability under the ECPA.

The purpose of the ECPA is to control conditions under which the interception of oral and wire communications will be permitted in order to safeguard their privacy. *Lam Lek Chong v. U.S. Drug Enforcement Admin.*, C.A.D.C.1991, 929 F.2d 729, 289 U.S.App.D.C. 136. The ECPA mandates that law enforcement shall receive a proper judicial authorization before intercepting any wire, oral or electronic communication. See 18 U.S.C. §2518. Under the ECPA, "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. 18 USC § 2510(4). The ECPA defines "contents" of electronic communications[8] to include any information concerning the substance, purport, or meaning of that communication. Title 18 U.S.C. § 2510(8).

The only information logged by law enforcement is the IP address; date; time; and key (hash value of the file). Law enforcement's actions on Freenet are similar to telephone traces. Telephone traces do not interfere with or observe the contents of dialogues, but merely trace source of communications, and, thus, do not constitute "interceptions" of communications as proscribed by the ECPA. *U.S. v. Seidlitz,* C.A.4 (Md.) 1978, 589 F.2d 152, certiorari denied 99 S.Ct. 2030, 441 U.S. 922, 60 L.Ed.2d 396. Law Enforcement on Freenet are collecting data as

[8] The ECPA defines "electronic communication" to mean any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. Title 18 U.S.C. § 2510(14).

an intended receipt, and therefore, as a party to the communication, which is not in violation of ECPA. 18 U.S.C. §2511(2)(c).

Courts have held that basic user identification information on the Internet is not content of communications. See *In re Zynga Privacy Litigation*, where the Court found that header information, which included a social network user's unique ID and the address of the webpage from which the user's request to view another webpage was sent, did not constitute the contents of any communication under the ECPA, and thus a social networking company and a social gaming company did not violate the ECPA by disclosing referer header information to third-party advertisers, even if a third-party could use the information to uncover the user's profile page and any personal information made available to the public on that page. *Id.*, C.A.9 (Cal.) 2014, 750 F.3d 1098.

Whether or not, a request on Freenet is determined to be "content" information, other peer nodes on Freenet are a parties to the communication because they are intended receipts of requests. The ECPA statute specifically exempts anyone who is a "party" to the communications. 18 U.S.C. §2511(2)(c). In this case, the law enforcement node on Freenet is a party to the communication since the defendant sent the request to the law enforcement node, then the node had to review the communication, determined it did not have the requested block, and sent out a new request for that file block. All of the actions taken by the law enforcement node to process the defendant's request make it a "party" to the communications and, therefore, excepted from liability under the ECPA.

Similarly, the action of a party to a telephone conversation in recording the conversation with defendant was an "interception" within statutory definition under this chapter, but did not

violate the ECPA, which specifically exempts situations in which one party to the conversation is the interceptor. *U.S. v. Turk*, C.A.5 (Fla.) 1976, 526 F.2d 654, rehearing denied 529 F.2d 523, certiorari denied 97 S.Ct. 74, 429 U.S. 823, 50 L.Ed.2d 84. Also see, *Smith v. Cincinnati Post and Times-Star*, which found that there is no "interception" or "eavesdropping" when a party to a conversation, or third person acting with consent of one of parties to the conversation, records that conversation. *Smith v. Cincinnati Post and Times-Star*, C.A.6 (Ohio) 1973, 475 F.2d 740. Therefore, even if the Court were to find that the mere logging of basic information from requestors on Freenet was an "interception," law enforcement is still not in violation of the ECPA because they were a party to the communication.

SI Becker was merely logging information that was coming to his node on Freenet. No substance of any communication was intercepted by SI Becker. Further, even if the Court were to find that SI Becker had intercepted communication and obtained content, his node was a party to the communication. The requests were sent out by defendant's node to his peer nodes, which included the law enforcement node, and made law enforcement a party to the communication. A party to the communication is excepted from violating the ECPA. It is lawful for a party to a communication to record that communication under ECPA. SI Becker's logging of information as a party to the defendant's electronic communications is lawful.

ii. <u>The Stored Communications Act Was Not Violated By Law Enforcement</u>

The Stored Communications Act (hereafter "SCA"), Title 18 U.S.C. §§2701-2712 regulates how the government can obtain customer records and actual content of

communications from telephone companies, email providers, etc. Whenever the government seeks out stored email, it was must comply with the SCA, specifically §2703. In this case, the government did not seek out any stored communications belonging to the defendant. §2702(b)(1) of the SCA permits the disclosure of contents of a communication to the intended recipient. The SCA does not apply because law enforcement did not try and get any information electronic service provider ("ESP") or an Internet service provider ("ISP").

IV. CONCLUSION

Courts across the country have found that an individual does not have reasonable expectation of a privacy on a peer-to-peer file sharing network. SI Becker logged information from the defendant's unsolicited requests to his law enforcement node on Freenet. SI Becker's law enforcement node on Freenet was the intended recipient of the defendant's electronic communication. Neither the ECPA nor the SCA applies in this case because SI Becker was a party to the defendant's communication. The defendant's supplemental motion to suppress should be denied.

Respectfully submitted,

RICHARD G. CALLAHAN
United States Attorney
s/ Colleen Lang
COLLEEN LANG, 56872MO
Assistant United States Attorney
111 South 10th Street, Room 20.333
St. Louis, MO 63102
(314) 539-2200

CERTIFICATE OF SERVICE

I hereby certify that on January 27, 2017, the foregoing was filed electronically with the Clerk of the Court. The foregoing was emailed to counsel of record for the defendant.

s/ Colleen Lang
COLLEEN LANG, 56872MO
Assistant United States Attorney